Computer networking and security research paper

Dhiali , Chetty, 231299

Open Window, School of Fundamentals

Interactive Development DV200

Tsungai Katsuro

10, June, 2025

Table of Contents

Introduction

In today's interconnected digital landscape, securing network communications is paramount to protect sensitive data from unauthorized access, interception and cyber threats. As organizations increasingly rely on networked systems, robust security frameworks become essential to maintain confidentiality, integrity and availability of information. This paper explores critical components of network security including cryptographic techniques, authentication protocols, access control models and security best practices through a review of academic literature and practical case studies. The goal is to present a comprehensive, evidence-based framework for enhancing network communication security.

Literature Review

1 Cryptographic Techniques

Cryptography is fundamental for protecting data in transit and at rest. Symmetric encryption algorithms such as the Advanced Encryption Standard (AES) employ a shared secret key for encryption and decryption, providing efficiency suitable for high-throughput data (Katz & Lindell, 2014). Conversely, asymmetric encryption, exemplified by RSA, uses a public-private key pair to facilitate secure key exchange over unsecured networks (Menezes, van Oorschot, & Vanstone, 1996). Hybrid encryption protocols combine these methods by using asymmetric cryptography to exchange symmetric session keys, thereby achieving both security and performance optimization.

Hash functions like SHA-256 generate unique fixed-length hash values to verify data integrity and authenticate message origins. These are critical in digital signatures and password management (Dang, 2015).

2 Authentication Mechanisms

Authentication mechanisms validate user identity to prevent unauthorized access. Traditional methods rely on passwords and PINs but contemporary systems increasingly utilize biometrics, smart cards and hardware tokens for enhanced security (Goodrich & Tamassia, 2014). Multi Factor authentication (MFA), which requires multiple verification factors such as knowledge (password), possession (token) and inherence (biometrics) significantly reduces risk of credential compromise.

Protocols like Kerberos utilize time-stamped tickets within trusted domains to authenticate users, while OAuth facilitates secure token-based authorization for third-party applications without exposing user credentials (Goodrich & Tamassia, 2014).

3 Access Control Models

Access control enforces restrictions on user permissions to resources. Discretionary Access Control (DAC) grants owners flexibility in assigning permissions but is vulnerable to misconfiguration (Ferraiolo & Kuhn, 1992). Mandatory Access Control (MAC) applies strict centralized policies based on data classifications, ideal for high-security contexts such as government or military networks (Ferraiolo & Kuhn, 1992).

Role-Based Access Control (RBAC) assigns permissions based on predefined roles, improving manageability and scalability in enterprise environments (Sandhu, Coyne, Feinstein, & Youman, 1996). RBAC supports efficient administration of complex access policies aligning user privileges with organizational responsibilities.

4 Security Practices

Effective network security depends on layered defenses:

- Firewalls regulate traffic based on predetermined rules to block unauthorized access.
- Intrusion Detection Systems (IDS) monitor networks for suspicious activities and raise alerts (Whitman & Mattord, 2018).
- Patch Management ensures timely updates to mitigate known vulnerabilities.
- Security Awareness Training equips users to recognize and respond to phishing, social engineering and other human-centric threats (Whitman & Mattord, 2018).

Access Control Assessment

In a simulated enterprise environment, three primary access control models (Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC)) were evaluated to determine their effectiveness in balancing security, flexibility and administrative efficiency.

Discretionary Access Control (DAC) offers a user-centric approach, allowing data owners to determine access permissions for other users. This model provides high flexibility particularly in collaborative environments where users need to share files or resources. However, this flexibility also introduces significant security risks especially in large organizations where users may unintentionally grant access to unauthorized individuals. Such user-driven permission settings often lead to inconsistent access controls increasing the risk of data leakage or insider threats. For example, in a DAC model a junior employee in HR could mistakenly grant access to sensitive employee records to someone outside the department violating confidentiality standards (Whitman & Mattord, 2018).

Mandatory Access Control (MAC), in contrast, enforces a centralized system-governed policy where users cannot alter access permissions. Data is classified (e.g. Confidential,

Secret, Top Secret) and access is granted based on security clearances and classification levels. MAC provides robust security controls making it ideal for environments requiring strict confidentiality such as government or military systems. However, MAC's rigidity makes it unsuitable for dynamic enterprise environments where rapid adaptation and collaboration between departments are required. The inability of end-users or department heads to adjust access levels on demand can slow productivity and increase administrative burdens.

Role-Based Access Control (RBAC) emerged as the most effective and scalable solution in the simulated environment. RBAC allows administrators to assign permissions to roles rather than individual users. Users are then granted access based on their assigned roles aligning access rights with job responsibilities. This not only enhances security by implementing the principle of least privilege but also streamlines administration by simplifying access management across departments. For instance, in an organization the Human Resources department can be assigned a role with access to employee records and recruitment systems while the Finance department has a separate role granting access to budgeting and payroll systems. The IT department may have elevated access to system logs and network tools. This segmentation ensures that individuals only access data necessary for their functions, minimizing exposure and reducing the risk of both accidental and intentional misuse (Sandhu et al., 1996).

Additionally, RBAC supports hierarchical roles, constraints and separation of duties which are features critical to mitigating fraud and improving accountability. For example, one user may be allowed to initiate financial transactions while a separate role must approve them. This layered control further reinforces organizational security while maintaining operational efficiency (Ferraiolo et al., 2001).

RBAC also enhances compliance with regulatory frameworks such as GDPR, HIPAA and ISO/IEC 27001 which require tight access control and auditability. Centralized role definitions allow for easier reporting, policy enforcement and system audits.

Security Practices Evaluation

To evaluate the effectiveness of security practices in a real-world enterprise environment this report examines the 2019 Capital One data breach, a significant cyberattack that compromised the sensitive data of over 100 million customers in the United States and Canada. This case offers insight into the deployment of firewalls, intrusion detection systems (IDS) and identity and access management (IAM) within a modern cloud-based infrastructure. The analysis is grounded in the detailed case study conducted by Novaes Neto, Madnick, Paula and Borges (2020).

- Firewall and Perimeter Defense Assessment

Capital One operated within Amazon Web Services (AWS) and utilized AWS's Web Application Firewall (WAF) as a critical perimeter defense. However, a misconfigured WAF rule allowed the attacker to exploit a Server-Side Request Forgery (SSRF) vulnerability enabling unauthorized access to the AWS EC2 metadata service. This misstep provided temporary security credentials which the attacker then used to access confidential data in Amazon S3 storage buckets. As noted by Novaes Neto et al. (2020), this configuration failure directly undermined the effectiveness of Capital One's perimeter defenses and illustrated the challenges of securing dynamic cloud environments.

- Intrusion Detection and Monitoring

Although Capital One employed security logging tools like AWS CloudTrail they lacked real-time alerting and internal network traffic analysis capable of identifying lateral movement. The breach went undetected internally for months and was only reported after a third-party security researcher alerted the company. According to Novaes Neto et al. (2020) this failure pointed to an overreliance on cloud-native logs without the proper implementation of advanced behavioral analysis or cross-platform correlation, weakening the efficacy of intrusion detection systems.

- Identity and Access Management (IAM)

A core security flaw in the breach was the attacker's access to an over-permissioned IAM role which violated the principle of least privilege. Once access was gained the attacker was able to exfiltrate data without restriction from multiple storage buckets. The case study by Novaes Neto et al. (2020) emphasizes that Capital One's access control configurations lacked granular policy enforcement and periodic privilege audits, which are vital in mitigating insider threats and credential misuse in cloud environments.

Strengths Identified:

- Use of cloud-native security tools (AWS WAF, CloudTrail).
- Deployment of scalable and flexible cloud infrastructure.
- Established vulnerability disclosure mechanisms that enabled third-party reporting.

Weaknesses Identified:

- Misconfigured WAF rules permitted metadata access via SSRF.
- Over-permissioned IAM roles violated the principle of least privilege.
- Lack of robust, real-time monitoring and anomaly detection tools.
- Infrequent security audits and delayed breach detection.
- Weak internal segmentation and privilege boundary enforcement.

Recommendations for Improvement:

- Harden WAF Configurations: Implement strict outbound rules to block unauthorized requests to internal services, particularly the EC2 metadata endpoint.
- Enforce Least Privilege Principles: IAM roles should be strictly scoped with automatic role expiration and subject to frequent reviews to eliminate excessive access rights.

- Adopt Real-Time Detection and Response Capabilities: Integrate cloud-native tools (like AWS GuardDuty) with third-party SIEMs and machine learning–based threat analytics to identify suspicious activity in real-time.
- Regular Security Posture Reviews: Conduct regular audits and penetration testing to uncover hidden misconfigurations and assess the efficacy of existing policies and controls.
- Enhance Training for DevSecOps Teams: Educate developers and operations teams on secure cloud deployment practices emphasizing risks such as SSRF and over-permissioning.
- Implement Microsegmentation and Access Boundaries: Isolate critical systems and data stores with fine-grained network segmentation to contain potential breaches.

The Capital One breach serves as a cautionary tale about the complexity of securing cloud environments. Despite having technically advanced systems in place the failure to enforce least privilege, misconfigured firewall rules and insufficient real-time monitoring created significant vulnerabilities. This incident highlights the need for organizations to treat cloud security as a shared responsibility and invest in both automated controls and human oversight. As Novaes Neto et al. (2020) conclude, the breach was less a failure of technology and more a failure of policy and configuration, a lesson critical for all enterprises navigating digital transformation.

Research Analysis and Recommendations

Drawing from literature and practical evaluations the following recommendations are proposed to strengthen network communication security:

- Adopt Hybrid Encryption: Combining AES for bulk data encryption with RSA for secure key exchange optimizes security and efficiency (Katz & Lindell, 2014; Menezes et al., 1996).

- Enforce Multifactor Authentication: MFA substantially lowers unauthorized access risks by requiring multiple verification layers (Goodrich & Tamassia, 2014).
- Implement Role-Based Access Control: RBAC provides scalable and manageable permission frameworks aligned with organizational structures (Sandhu et al., 1996).
- Regularly Audit Firewalls and IDS: Periodic reviews ensure security configurations remain effective against evolving threats (Whitman & Mattord, 2018).
- Invest in Cybersecurity Training: Continuous user education reduces susceptibility to social engineering attacks.
- Leverage AI and Machine Learning: Adaptive threat detection and behavioral analytics improve responsiveness to emerging threats.
- Utilize Blockchain for Data Integrity: Distributed ledgers provide tamper-evident logging and secure data sharing.

A holistic implementation combining these strategies with policy enforcement and user engagement is critical for resilient network security.

Conclusion

Securing network communications necessitates a multifaceted and integrated approach combining robust cryptographic techniques, reliable authentication mechanisms, structured access control and proactive security practices. This research has examined theoretical principles alongside real-world applications to formulate a comprehensive understanding of network security.

The literature affirms the effectiveness of hybrid cryptographic systems, multifactor authentication and role-based access control in strengthening digital defenses. Moreover, the evaluation of security practices emphasizes the need for layered defense strategies, regular system updates and user education.

In response to emerging threats and evolving infrastructures, organizations must adopt adaptable and forward-thinking security frameworks. This includes leveraging artificial intelligence for threat detection, adopting blockchain for integrity assurance and enforcing stringent access and monitoring protocols. By aligning technological solutions with organizational policies institutions can enhance the resilience and trustworthiness of their networks.

Annexure A: Case Study Analysis

ARP Spoofing and Network Exploitation in the 2013 Target Corporation Data Breach

Introduction

The 2013 Target Corporation data breach remains one of the most significant cybersecurity incidents in retail history. It exposed the personal and financial information of tens of millions of consumers and highlighted deep flaws in cybersecurity governance, network architecture and vendor access control. This case study analyzes the technical and organizational weaknesses that enabled the attack focusing specifically on ARP spoofing, lateral movement and memory scraping techniques as discussed in the unpublished manuscript by Yao and Shin (n.d.). Through this lens, the case provides valuable lessons for building secure and resilient information systems in complex enterprise environments.

Background

In November 2013 attackers infiltrated Target’s network by stealing credentials from a third-party HVAC vendor. These credentials granted the attackers access to Target's business network which critically was not adequately segmented from the payment processing network. Once inside, the attackers performed ARP (Address Resolution Protocol) spoofing to redirect traffic within the internal network and to facilitate the installation of RAM-scraping malware on point-of-sale (POS) terminals.

This malware extracted unencrypted payment card information as it passed through the memory of infected POS devices. Despite multiple security alerts, some triggered by a FireEye intrusion detection system, the breach went undetected for weeks. The attack resulted in the compromise of approximately 40 million credit and debit card records and 70 million records of personal information including names, addresses, phone numbers and email addresses (Yao & Shin, n.d.).

Identified Vulnerabilities

- Over-permissioned Vendor Access: The HVAC vendor was granted access far beyond what was necessary for its operational functions. This violated the principle of least privilege, exposing sensitive segments of the internal network to third parties. The attackers exploited this to gain a foothold.
- Lack of Network Segmentation: Target's internal network was flat allowing attackers to move laterally from non-critical systems to sensitive infrastructure like the POS environment. Proper segmentation (e.g. VLANs or firewalls) could have isolated payment systems from vendor-accessible zones.
- ARP Spoofing Vulnerability: The network lacked controls to prevent ARP spoofing enabling attackers to intercept and manipulate internal communications. By sending forged ARP messages they redirected traffic and escalated their access privileges within the system.
- Unencrypted Card Data in Memory: POS devices processed cardholder data in plaintext in memory (RAM) making it vulnerable to RAM scraping malware. This design flaw allowed attackers to extract sensitive data with ease once the malware was deployed.
- Ineffective Intrusion Detection and Response: Although Target had deployed FireEye and other security tools that detected anomalies and flagged the malware alerts were either ignored or not escalated. There was a clear breakdown in the incident response workflow and accountability.

- Lack of Timely Patching and Security Audits: Target failed to implement timely security patches and conduct frequent audits that could have detected vulnerabilities in vendor access, traffic anomalies and malware signatures.

Implications

- Financial Repercussions: Target incurred losses exceeding $162 million due to legal settlements, credit monitoring for affected customers, payment card reissuance, forensic investigations and system upgrades.These costs excluded intangible losses such as diminished customer trust (Yao & Shin, n.d.).
- Reputational Damage: The breach severely impacted Target's brand image especially during the peak holiday shopping season. It undermined consumer confidence in the company's ability to safeguard sensitive data and resulted in public and media scrutiny.
- Organizational Consequences: Senior executives including the Chief Information Officer (CIO) and Chief Executive Officer (CEO) resigned following the breach. This prompted internal restructuring and a re-evaluation of the company's cybersecurity leadership and strategy.
- Legal and Regulatory Fallout: Target faced multiple lawsuits and regulatory investigations by state attorneys general and federal agencies. It agreed to settlements that required adopting stricter cybersecurity measures and submitting to ongoing compliance audits.
- Industry-wide Wake-Up Call: The breach became a catalyst for industry-wide reform especially in retail. Companies began enforcing stricter third-party access controls, tokenization of payment data and real-time security analytics. It also fueled the shift from magnetic stripe cards to EMV (chip-and-PIN) cards in the U.S.

Recommendations

- Enforce Network Segmentation: Implement robust network segmentation to isolate payment processing environments from third-party accessible systems. Use VLANs, firewalls and access control lists to prevent lateral movement by unauthorized users.
- Deploy Dynamic ARP Inspection (DAI): Configure DAI on switches to detect and block ARP spoofing attempts. This protocol validates ARP packets against trusted bindings neutralizing the attacker's ability to reroute internal traffic.
- Restrict and Monitor Vendor Access: Apply strict Role-Based Access Control (RBAC) and enforce just-in-time access provisioning for third-party vendors. All vendor sessions should be monitored, logged and terminated after task completion.
- Encrypt Card Data in Memory and Transit: Use end-to-end encryption for cardholder data ensuring that it is protected at all stages, from swipe/tap to storage. Also use tokenization to replace card data with randomly generated tokens.
- Strengthen Incident Detection and Response: Build a mature Security Operations Center (SOC) with 24/7 monitoring. Ensure that alerting systems have clearly defined escalation paths and that all alerts are promptly investigated by trained personnel.
- Conduct Frequent Security Audits and Penetration Testing: Perform regular penetration tests and vulnerability assessments across all networks and applications. Include third-party systems in audit scopes to proactively identify and remediate potential entry points.
- Cybersecurity Awareness Training: Educate internal teams and vendors on best practices, social engineering threats and secure access protocols. Human error remains a common vulnerability especially in credential security.

This case underscores the importance of implementing a defense-in-depth security strategy where multiple layers of protection (technical, procedural and administrative) mitigate the risk of a breach. The failure of Target's intrusion detection, vendor management and network architecture demonstrates how security must be both comprehensive and coordinated. It also reflects the growing relevance of zero-trust principles where no actor, internal or external, is inherently trusted.

The Target breach is not just a failure of technology but of organizational prioritization and responsiveness. Despite having advanced security tools in place Target failed to act on critical alerts due to poor incident response planning. Additionally, their lack of basic network hygiene, such as segmentation and access control allowed relatively unsophisticated methods like ARP spoofing to become highly effective. This case illustrates how security is a holistic discipline requiring alignment between technology, policy and human action. Proactive investment in cyber defense is no longer optional, it is integral to business continuity.

References

Ferraiolo, D. F., & Kuhn, D. R. (1992). Computer Security Division, I.T.L. *Role based access control: CSRC*, *CSRC*. Available at: https://csrc.nist.gov/projects/role-based-access-control.

Goodrich, M. T., & Tamassia, R. (2014). *Introduction to computer security_ Goodrich Tamassia pearson new international edition (PDFDrive.com).PDF*, *pdfcoffee.com*. Available at:https://pdfcoffee.com/introduction-to-computer-security-goodrich-tamassia-pearson-new-international-edition-pdfdrivecom-pdf-2-pdf-free.html .

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of - applied cryptography*. Available at: https://galois.azc.uam.mx/mate/propaganda/Menezes.pdf .

Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). *A role-based access control model and reference implementation within a corporate intranet* | *ACM Transactions on Information and System Security*. Availableat:https://dl.acm.org/doi/10.1145/300830.300834.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security 6th edition*, *pdfcoffee.com*. Available at: https://pdfcoffee.com/principles-of-information-security-6th-edition-pdf-free.html .

Novaes Neto, Nelson & Madnick, Stuart & Paula, Anchises & Borges, Natasha. (2020). A Case Study of the Capital One Data Breach. SSRN Electronic Journal. 10.2139/ssrn.3542567.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). *Proposed NIST standard for role-based access control*. Available at: https://profsandhu.com/journals/tissec/p224-ferraiolo.pdf.

Yao, D., & Shin, R. (n.d.). *Case study: Target data breach*. Unpublished manuscript. Available at: https://people.cs.vt.edu/danfeng/papers/Target-Yao-unpublished.pdf .

Dang, Q. H. (2015). *Secure Hash Standard (SHS)* (FIPS PUB 180-4). National Institute of Standards and Technology. *NIST*. Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography, Second edition*. Available at:https://eclass.uniwa.gr/modules/document/file.php/CSCYB105/Reading%20Material/%5BJonathan_Katz,_Yehuda_Lindell%5D_Introduction_to_Mo(2nd).pdf.